WHAT IS CLAIMED IS

1. A method for embedding a message within a file, comprising:

generating a random key;

encrypting the random key to produce an encrypted random key;

encrypting the message to produce an encrypted message; and

embedding the encrypted random key and the encrypted message in the file, at least one of the encrypted random key and the encrypted message being embedded in random locations throughout the file.

2. The method of claim 1, wherein the generating includes:

generating a random symmetric encryption key.

3. The method of claim 1, wherein the encrypting the random key includes:

asymmetrically encrypting the random key with an intended recipient's public key.

4. The method of claim 2, wherein the encrypting the message includes:

symmetrically encrypting the message with the random symmetric encryption key.

5. The method of claim 1, further comprising:

compressing the message to obtain a compressed message prior to the encrypting the message.

6. The method of claim 5, further comprising:

encrypting a length of the encrypted message with the random key to obtain an encrypted message length.

7. The method of claim 6, further comprising:

verifying that the file has sufficient capacity to contain the encrypted message length, the encrypted random key, and the encrypted message.

8. The method of claim 1, wherein the embedding includes:

randomly embedding both the encrypted random key and the encrypted message throughout the file

9. The method of claim 1, wherein the embedding includes:

seeding a random number generator with an intended recipient's public key, and supplementally seeding the random number generator with the random key.

10. The method of claim 9, wherein the embedding further includes:

embedding the encrypted random key at locations in the file corresponding to random numbers generated by the random number generator after the seeding the random number generator with the intended recipient's public key.

11. The method of claim 9, wherein the embedding further includes:

embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after the supplementally seeding the random number generator with the random key.

12. A method for embedding a message within a file, comprising:

compressing the message to produce a compressed message;

generating a random key;

encrypting the random key with a public key to produce an encrypted random key;

encrypting the compressed message with the random key to produce an encrypted message;

encrypting a length of the encrypted message with the random key to produce an encrypted message length;

seeding a random number generator; and

embedding the encrypted random key, the encrypted message length, and the encrypted message in the file, at least one of the encrypted random key, the encrypted message length, and

the encrypted message being embedded in locations throughout the file corresponding to random numbers produced by the random number generator.

13. The method of claim 12, further comprising:

verifying that the file has sufficient capacity to contain the encrypted message length, the encrypted random key, and the encrypted message.

14. The method of claim 12, wherein the embedding includes:

embedding each of the encrypted random key, the encrypted message length, and the encrypted message in locations throughout the file corresponding to random numbers produced by the random number generator.

15. The method of claim 12, wherein the seeding includes:

seeding the random number generator with the public key, and

supplementally seeding the random number generator with the random key.

16. The method of claim 15, wherein the supplementally seeding causes the random number generator to produce numbers based on both the random key and a state of the random number generator at a time of the supplementally seeding.

17. The method of claim 15, wherein the embedding further includes:

embedding the encrypted random key at locations in the file corresponding to random numbers generated by the random number generator after the seeding the random number generator with the public key.

18. The method of claim 15, wherein the embedding further includes:

embedding the encrypted message length at locations in the file corresponding to random numbers generated by the random number generator after the supplementally seeding the random number generator with the random key.

19. The method of claim 15, wherein the embedding further includes:

embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after the supplementally seeding the random number generator with the random key, the embedding the encrypted message occurring until a total number of bits embedded equals a predetermined percentage of available space within the file.

20. The method of claim 19, wherein the embedding further includes:

embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the predetermined percentage of available space within the file.

21. A method for embedding a message within a file, comprising:

generating a session key;

encrypting the session key with a public key to produce an encrypted session key;

encrypting the message with the session key to produce an encrypted message;

seeding a random number generator with the public key;

embedding the encrypted session key throughout the file in locations corresponding to random numbers produced by the random number generator;

seeding the random number generator with the session key;

and

embedding the encrypted message throughout the file in locations corresponding to random numbers produced by the random number generator after the seeding with the session key.

22. The method of claim 21, further comprising:

encrypting a length of the encrypted message with the session key to produce an encrypted message length; and

embedding the encrypted message length throughout the file in locations corresponding to random numbers produced by the random number generator after the seeding with the session key.

23. The method of claim 21, wherein the embedding the encrypted message includes:

embedding the encrypted message at locations in the file corresponding to random numbers generated by the random number generator after the seeding the random number generator with the session key, the embedding the encrypted message occurring until a total number of bits embedded in the file equals a determined percentage of available space within the file.

24. The method of claim 23, wherein the embedding the encrypted message further includes:

embedding the encrypted message at sequential unused locations in the file when the total number of bits embedded exceeds the determined percentage of available space within the file.

25. The method of claim 23, wherein the determined percentage is a fixed percentage.

26. The method of claim 23, further comprising:

randomly determining the determined percentage.

27. A computer-readable medium that stores instructions executable by one or more processors to embed a message within a file, comprising:

instructions for generating a random session key;

instructions for encrypting the session key to produce an encrypted session key;

instructions for encrypting the message to produce an encrypted message;

instructions for seeding a random number generator;

instructions for randomly embedding the encrypted session key throughout the file in locations corresponding to random numbers produced by the random number generator;

instructions for re-seeding the random number generator;

and

instructions for embedding the encrypted message throughout the file in locations corresponding to random numbers produced by the random number generator after the re-seeding.

28. A processing device, comprising:

a processor; and

a memory operatively coupled to the processor and containing a message, a file, and instructions which when executed by the processor perform the functions of:

generating a random key,

encrypting the random key to produce an encrypted random key,

encrypting the message to produce an encrypted message, and

embedding the encrypted random key and the encrypted message in the file, at least one the encrypted random key and the encrypted message being embedded in random locations throughout the file.